

FROM NEIGHBOUR TRANSITIVE CODES TO FREQUENCY PERMUTATION ARRAYS

NEIL I. GILLESPIE AND CHERYL E. PRAEGER

ABSTRACT. Constant composition codes have been proposed as suitable coding schemes to solve the narrow band and impulse noise problems associated with powerline communication. In particular, a certain class of constant composition codes called frequency permutation arrays have been suggested as ideal, in some sense, for these purposes. In this paper we characterise a family of neighbour transitive codes in Hamming graphs, and show that the only constant composition codes that can appear in this family are frequency permutation arrays, providing an infinitely family of examples.

1. INTRODUCTION

Powerline communication has been proposed as a solution to the “last mile problem” in the delivery of reliable telecommunications at the lowest cost [7, 10]. Any coding scheme designed for powerline communication must deal with a *permanent narrow band noise* and an *impulse noise*, as well as the usual white Gaussian/background noise [2, 7, 10]. The authors introduced *neighbour transitive codes* (see Definition 2.4) as a group theoretic analogue to the assumption that white Gaussian noise affects symbols in codewords independently at random [4]; an assumption often made in error correction coding theory [11, p.5]. A *constant composition code* (CCC) of length m over an alphabet Q of size q has the property that each codeword has p_i occurrences of the i^{th} letter of the alphabet, where the p_i are positive integers such that $\sum p_i = m$, and such codes have been proposed as suitable coding schemes to deal with the extra noise considerations in powerline communication [2, 3]. It is suggested in [2] that constant composition codes where the p_i are roughly the same for all i are particularly well suited for powerline communication. Constant composition codes where each letter occurs p times in each codeword are called *frequency permutation arrays*, and were introduced in [8].

In this paper, we consider codes of length m over an alphabet Q of size q to be subsets of the vertices of the Hamming graph $H(m, q)$. The automorphism group of $H(m, q)$, denoted by $\text{Aut}(\Gamma)$, is equal to the semi-direct product $\mathfrak{B} \rtimes \mathfrak{L}$, where $\mathfrak{B} \cong S_q^m$ and $\mathfrak{L} \cong S_m$ (see Section 2 for descriptions of how these groups act on vertices of $H(m, q)$). We define the *automorphism group of a code* C to be the setwise stabiliser in $\text{Aut}(\Gamma)$ of C , and denote it by $\text{Aut}(C)$. Let α be a vertex in $H(m, q)$, and suppose

Date: draft typeset March 2, 2013

2000 Mathematics Subject Classification: 05E20, 20B25, 94B60.

Key words and phrases: powerline communication, constant composition codes, frequency permutation arrays, neighbour transitive and completely transitive codes .

$\{a_1, \dots, a_k\}$ is the set of letters that occur in α . The *composition of a codeword* α is the set

$$(1) \quad Q(\alpha) = \{(a_1, p_1), \dots, (a_k, p_k)\},$$

where there are exactly $p_i > 0$ occurrences of the letter a_i in the codeword α . It follows from the definition of a constant composition code that $Q(\alpha) = Q(\beta)$ for all codewords α, β . Therefore, we can talk of the *composition of a constant composition code*, which is equal to $Q(\alpha)$ for each codeword α . It follows that any automorphism of a CCC must leave the composition invariant. For $\sigma \in \mathfrak{L}$, the image α^σ is just a rearrangement of the letters occurring in α , so $Q(\alpha) = Q(\alpha^\sigma)$ for all $\sigma \in \mathfrak{L}$ and any vertex α . If we consider automorphisms from \mathfrak{B} that fix $Q(\alpha)$ the situation is more complicated. For example, for graph automorphisms of the form $x = (h, \dots, h)$ for some $1 \neq h \in S_q$, we prove (see Lemma 2.10) that if $Q(\alpha)$ is as in (1) then

$$Q(\alpha^x) = \{(a_1^h, p_1), \dots, (a_k^h, p_k)\}.$$

Thus, if $Q(\alpha^x) = Q(\alpha)$ then there exist $i \neq j$ such that $p_i = p_j$. Indeed, for α in a frequency permutation array, $p_i = p_j$ for all i, j and $Q(\alpha^x) = Q(\alpha)$. If $m = pq$ for some positive integer p , we define $\text{All}(pq, q)$ to be the code consisting of all codewords in which every letter from Q appears exactly p times. That is, $\text{All}(pq, q)$ is the largest possible frequency permutation array over Q of length pq . We prove that $\text{All}(pq, q)$ is $\text{Aut}(C)$ -neighbour transitive, and that $\text{Aut}(C) = \text{Diag}_m(S_q) \rtimes \mathfrak{L}$, where $\text{Diag}_m(S_q) = \{(h, \dots, h) \in \mathfrak{B} : h \in S_q\}$ (Theorem 3.2). Given that the composition of a constant composition code is invariant under the automorphism group of the code, it is natural to ask what other X -neighbour transitive constant composition codes exist with $X \leq \text{Diag}_m(S_q) \rtimes \mathfrak{L}$. It turns out that such codes are necessarily frequency permutation arrays, as our main result shows.

Theorem 1.1. *Let C be an X -neighbour transitive code in $H(m, q)$ with $X \leq \text{Diag}_m(S_q) \rtimes \mathfrak{L}$. Then either C is a frequency permutation array; $C = \{(a, \dots, a)\}$ for some $a \in Q$; or C is one of the codes described in Definition 3.1 (i), (ii) or (iii) (none of which is a constant composition code).*

In Section 2 we introduce the required definitions and some preliminary results. Then, in Section 3 we introduce the codes $\text{Rep}(m, q)$, $W([m/2], 2)$, $\text{Diff}(m, q)$ and $\text{All}(pq, q)$, and prove that each is neighbour transitive with automorphism group $\text{Diag}_m(S_q) \rtimes \mathfrak{L}$. In the final section we prove some results about connected subsets of the set of vertices in $H(m, q)$ and use these results to prove Theorem 1.1.

2. DEFINITIONS AND PRELIMINARIES

The *Hamming graph* $H(m, q)$ is the graph Γ with vertex set $V(\Gamma)$, the set of m -tuples with entries from an *alphabet* Q of size q , and an edge exists between two vertices if and only if they differ in precisely one entry. Throughout we assume that $q, m \geq 2$. Any code of length m over an alphabet Q of size q can be embedded as a subset of the vertex set of $\Gamma = H(m, q)$. The automorphism group of $H(m, q)$, which we denote by $\text{Aut}(\Gamma)$, is the semi-direct product $\mathfrak{B} \rtimes \mathfrak{L}$ where $\mathfrak{B} \cong S_q^m$ and $\mathfrak{L} \cong S_m$, see [1, Theorem 9.2.1]. Let $g = (g_1, \dots, g_m) \in \mathfrak{B}$, $\sigma \in \mathfrak{L}$ and $\alpha = (\alpha_1, \dots, \alpha_m) \in V(\Gamma)$. Then g and σ acts on α in the following way:

$$\alpha^g = (\alpha_1^{g_1}, \dots, \alpha_m^{g_m}) \quad \alpha^\sigma = (\alpha_{1\sigma^{-1}}, \dots, \alpha_{m\sigma^{-1}}).$$

We define the following subgroup of \mathfrak{B} :

$$\text{Diag}_m(S_q) := \{(h, \dots, h) \in \mathfrak{B} : h \in S_q\}.$$

Let $M = \{1, \dots, m\}$, and view M as the set of vertex entries of $H(m, q)$. Let 0 denote a distinguished element of the alphabet Q . For $\alpha \in V(\Gamma)$, the *support* of α is the set $\text{supp}(\alpha) = \{i \in M : \alpha_i \neq 0\}$. The *weight* of α is defined as $\text{wt}(\alpha) = |\text{supp}(\alpha)|$. In the case of the binary Hamming graph (that is, $q = 2$), the *complement* of α , denoted by α^c , is the unique vertex in $H(m, 2)$ with $\text{supp}(\alpha^c) = M \setminus \text{supp}(\alpha)$. For all pairs of vertices $\alpha, \beta \in V(\Gamma)$, the *Hamming distance* between α and β , denoted by $d(\alpha, \beta)$, is defined to be the number of entries in which the two vertices differ. We let $\Gamma_k(\alpha)$ denote the set of vertices in $H(m, q)$ that are at distance k from α .

Let $\alpha = (\alpha_1, \dots, \alpha_m) \in V(\Gamma)$. For $a \in Q$ we let $\nu(\alpha, i, a) \in V(\Gamma)$ denote the vertex where the j -entry satisfies

$$\nu(\alpha, i, a)|_j = \begin{cases} \alpha_j & \text{if } j \neq i \\ a & \text{if } j = i. \end{cases}$$

We note that if $\alpha_i = a$ then $\nu(\alpha, i, a) = \alpha$, otherwise $\nu(\alpha, i, a) \in \Gamma_1(\alpha)$. Throughout this paper whenever we refer to $\nu(\alpha, i, a)$ as a *neighbour* of α , or being adjacent to α , we mean that $a \in Q \setminus \{\alpha_i\}$. Let us now consider how automorphisms act on vertices of the form $\nu(\alpha, i, a)$.

Lemma 2.1. *Let $\alpha = (\alpha_1, \dots, \alpha_m) \in V(\Gamma)$, $a \in Q$, and $x = (h_1, \dots, h_m)\sigma \in \text{Aut}(\Gamma)$. Then $\nu(\alpha, i, a)^x = \nu(\alpha^x, i^\sigma, a^{h_i})$, and is a neighbour of α^x if and only if $\nu(\alpha, i, a)$ is a neighbour of α .*

Proof. Let $h = (h_1, \dots, h_m) \in \mathfrak{B}$, so $x = h\sigma$. Then

$$\nu(\alpha, i, a)^h|_j = \begin{cases} \alpha_j^{h_j} & \text{if } j \neq i \\ a^{h_i} & \text{if } j = i \end{cases}$$

Since $\alpha^h|_j = \alpha_j^{h_j}$ for all j it follows that $\nu(\alpha, i, a)^h = \nu(\alpha^h, i, a^{h_i})$, and $a^{h_i} \neq \alpha^h|_i$ if and only if $a \neq \alpha_i$. Now suppose $k^\sigma = \ell$. Then

$$\nu(\alpha, i, a)^\sigma|_\ell = \nu(\alpha, i, a)|_k = \begin{cases} \alpha_k & \text{if } k \neq i \\ a & \text{if } k = i \end{cases} = \begin{cases} \alpha_{\ell^{\sigma^{-1}}} & \text{if } \ell \neq i^\sigma \\ a & \text{if } \ell = i^\sigma \end{cases}$$

Since $\alpha^\sigma|_\ell = \alpha_{\ell^{\sigma^{-1}}}$ for all ℓ it follows that $\nu(\alpha, i, a)^\sigma = \nu(\alpha^\sigma, i^\sigma, a)$, and $a \neq \alpha^\sigma|_{i^\sigma}$ if and only if $a \neq \alpha_i$. Applying σ to $\nu(\alpha^h, i, a^{h_i})$, we conclude that $\nu(\alpha, i, a)^x = \nu(\alpha^x, i^\sigma, a^{h_i})$ and $a^{h_i} \neq \alpha^x|_{i^\sigma}$ if and only if $a \neq \alpha_i$. \square

Definition 2.2. Let α and β be distinct vertices of $H(m, q)$. Define the following sets:

$$\begin{aligned} J(\alpha, \beta) &= \{i \mid \alpha_i \neq 0 \text{ and } \beta_i = 0\}, \\ S(\alpha, \beta) &= \{i \mid \alpha_i = \beta_i \text{ and } \alpha_i \neq 0\}, \\ D(\alpha, \beta) &= \{i \mid \alpha_i \neq \beta_i \text{ and } \alpha_i, \beta_i \neq 0\}. \end{aligned}$$

Note that $\text{supp}(\alpha) = J(\alpha, \beta) \cup S(\alpha, \beta) \cup D(\alpha, \beta)$. Furthermore, $J(\alpha, \beta)$ and $J(\beta, \alpha)$ are disjoint sets, $S(\alpha, \beta) = S(\beta, \alpha)$ and $D(\alpha, \beta) = D(\beta, \alpha)$.

Lemma 2.3. *Let α, β be vertices of weight t, k respectively with $t \leq k$. Suppose $|J(\alpha, \beta)| = j$ and $|S(\alpha, \beta)| = s$. Then $|D(\alpha, \beta)| = t - j - s$, $|J(\beta, \alpha)| = k - t + j$ and $d(\alpha, \beta) = k - s + j$. Furthermore, if $q = 2$ then $j + s = t$ and $d(\alpha, \beta) = |J(\alpha, \beta)| + |J(\beta, \alpha)|$.*

Proof. Because $\text{supp}(\alpha) = J(\alpha, \beta) \cup S(\alpha, \beta) \cup D(\alpha, \beta)$, it is clear that $d := |D(\alpha, \beta)| = t - j - s$. Thus $|J(\beta, \alpha)| = k - s - d = k - t + j$. Hence the number of entries where α and β differ is $|J(\beta, \alpha)| + |J(\alpha, \beta)| + |D(\alpha, \beta)| = k - t + j + j + t - j - s = k - s + j$. Suppose now that $q = 2$. Then $D(\alpha, \beta) = \emptyset$, and so $t - j - s = 0$. It follows that $|J(\alpha, \beta)| + |J(\beta, \alpha)| = k - s + j = d(\alpha, \beta)$. \square

Let C be a code in $H(m, q)$. The *minimum distance*, δ , of C is the smallest distance between distinct codewords of C . For any $\gamma \in V(\Gamma)$, we define the *distance of γ from C* to be

$$d(\gamma, C) = \min\{d(\gamma, \beta) : \beta \in C\}.$$

The *covering radius* of C , which we denote by ρ , is the maximum distance of any vertex in $H(m, q)$ from C . We let C_i denote the set of vertices that are distance i from C , and deduce, for $i \leq \lfloor (\delta - 1)/2 \rfloor$, that C_i is the disjoint union of $\Gamma_i(\alpha)$ as α varies over C . Furthermore, $C_0 = C$ and $\{C, C_1, \dots, C_\rho\}$ forms a partition of $V(\Gamma)$ called the *distance partition* of C . In particular, the *complete code* $C = V(\Gamma)$ has covering radius 0 and trivial distance partition $\{C\}$; and if C is not the complete code, we call the non-empty subset C_1 the *set of neighbours* of C . Let C and C' be codes in $H(m, q)$. We say C and C' are *equivalent* if there exists $x \in \text{Aut}(\Gamma)$ such that $C^x = C'$.

Definition 2.4. Let C be a code in $H(m, q)$ with distance partition $\{C, C_1, \dots, C_\rho\}$. We say C is *X-neighbour transitive*, or simply *neighbour transitive*, if there exists $X \leq \text{Aut}(\Gamma)$ such that C_i is an X -orbit for $i = 0, 1$. If there exists $X \leq \text{Aut}(\Gamma)$ such that C_i is an X -orbit for $i = 0, \dots, \rho$, we say C is *X-completely transitive*, or simply *completely transitive*.

Remark 2.5. The reader should note that the definition of neighbour transitive given in [4] is more general than the one given here in that it only requires C_1 to be an X -orbit. However, it is not unreasonable to use this definition as, if C_1 is an X -orbit, $\delta \geq 3$, and X fixes C setwise, then X necessarily acts transitively on C , and in [4] it is shown that X often fixes C setwise. One should also note that it follows from the definition above that any completely transitive code is necessarily neighbour transitive.

Lemma 2.6. *Let C be a code with distance partition $\mathcal{C} = \{C, C_1, \dots, C_\rho\}$ and $y \in \text{Aut}(\Gamma)$. Then $C_i^y := (C_i)^y = (C^y)_i$ for each i . In particular, the code C^y has distance partition $\{C^y, C_1^y, \dots, C_\rho^y\}$, and \mathcal{C} is $\text{Aut}(C)$ -invariant. Moreover, C is X -neighbour (completely) transitive if and only if C^y is X^y -neighbour (completely) transitive.*

Proof. Let $\beta \in C_i$. Then there exists $\alpha \in C$ such that $d(\beta, \alpha) = i$. Since automorphisms preserve adjacency it follows that $d(\beta^y, \alpha^y) = i$. Thus $d(\beta^y, C^y) \leq i$. The same argument shows that if $j = d(\beta^y, C^y)$ then $i = d(\beta, C) = d((\beta^y)^{y^{-1}}, (C^y)^{y^{-1}}) \leq j$, and hence $d(\beta^y, C^y) = i$. Thus $(C_i)^y \subseteq (C^y)_i$. A similar argument shows that $(C^y)_i \subseteq (C_i)^y$. Hence $(C_i)^y = (C^y)_i$. Therefore, without ambiguity, we can denote this set by C_i^y . Thus the distance partition of C^y is $\{C^y, C_1^y, \dots, C_\rho^y\}$. In particular, if $y \in \text{Aut}(C)$, it

follows that $(C_i)^y = (C^y)_i = C_i$ for each i . That is \mathcal{C} is $\text{Aut}(C)$ -invariant. Finally, C is X -neighbour (completely) transitive if and only if C_i is an X -orbit for $i = 0, 1$ ($i = 0, \dots, \rho$), which holds if and only if C_i^y is an X^y -orbit for $i = 0, 1$ ($i = 0, \dots, \rho$). \square

Definition 2.7. Let C be a code with covering radius ρ and let s be an integer such that $0 \leq s \leq \rho$. As in [1, p. 346], we say C is s -regular if for each vertex $\gamma \in C_i$, with $0 \leq i \leq s$, and integer $k = 0, \dots, m$, the number of codewords at distance k from γ depends only on i and k , and is independent of the choice of $\gamma \in C_i$. If $s = \rho$, we say C is *completely regular*.

Remark 2.8. It is known that completely transitive codes are necessarily completely regular [6, Lemma 2.1]. Similarly, because automorphisms preserve adjacency, it is straight forward to show that any neighbour transitive code is necessarily 1-regular.

Lemma 2.9. Let C be a completely regular code in $H(m, q)$ with distance partition $\{C, C_1, \dots, C_\rho\}$. Then C_ρ is completely regular with distance partition $\{C_\rho, C_{\rho-1}, \dots, C_1, C\}$; and $\text{Aut}(C) = \text{Aut}(C_\rho)$. Furthermore, C is X -completely transitive if and only if C_ρ is X -completely transitive.

Proof. The fact that C_ρ is completely regular with distance partition $\{C_\rho, C_{\rho-1}, \dots, C\}$ is given in [9]. Lemma 2.6 implies that $\text{Aut}(C) = \text{Aut}(C_\rho)$. Now suppose C is X -completely transitive. Then each C_i is an X -orbit, and hence C_ρ is X -neighbour transitive. The converse follows by a similar argument. \square

For $a_1, \dots, a_k \in Q$ and positive integers p_1, \dots, p_k such that $\sum p_i = m$, we let $(a_1^{p_1}, a_2^{p_2}, \dots, a_k^{p_k})$ denote the vertex

$$\underbrace{(a_1, \dots, a_1)}_{p_1}, \underbrace{(a_2, \dots, a_2)}_{p_2}, \dots, \underbrace{(a_k, \dots, a_k)}_{p_k} \in V(\Gamma)$$

For $\alpha \in V(\Gamma)$, recall $Q(\alpha)$, the composition of α , defined in (1). For each distinct p_i that appears in $Q(\alpha)$ we want to register the number of distinct letters that appear p_i times. We let

$$\text{Num}(\alpha) = \{(p_1, s_1), (p_2, s_2), \dots, (p_j, s_j)\}$$

where (p_i, s_i) means that s_i distinct letters appear p_i times in α . We note that $\sum s_i = k$, the number of distinct letters that occur in α .

Lemma 2.10. Let $\alpha \in V(\Gamma)$ with $Q(\alpha) = \{(a_1, p_1), \dots, (a_k, p_k)\}$ and let $x = (h, \dots, h)\sigma \in \text{Diag}_m(S_q) \rtimes \mathfrak{L}$. Then $Q(\alpha^x) = \{(a_1^h, p_1), \dots, (a_k^h, p_k)\}$ and $\text{Num}(\alpha^x) = \text{Num}(\alpha)$.

Proof. Let $\alpha = (\alpha_1, \dots, \alpha_m)$ and $a \in Q$. Note that $\alpha_i = a$ if and only if $(\alpha_i)^h = a^h$, and that $(\alpha_i)^h = \alpha^x|_{i\sigma}$. Therefore for every occurrence of a in α there is a corresponding occurrence of a^h in α^x . Thus $Q(\alpha^x) = \{(a_1^h, p_1), \dots, (a_k^h, p_k)\}$. We note that $\{p_1, \dots, p_k\}$ is left invariant by the action of x on α . Therefore $\text{Num}(\alpha) = \text{Num}(\alpha^x)$. \square

Corollary 2.11. Let C be an X -neighbour transitive code with $X \leq \text{Diag}_m(S_q) \rtimes \mathfrak{L}$, and let $\nu \in C_i$ for some $i = 0, 1$. Then $\text{Num}(\nu') = \text{Num}(\nu)$ for all $\nu' \in C_i$. If in addition $X \leq \mathfrak{L}$, then $Q(\nu') = Q(\nu)$ for all $\nu' \in C_i$.

3. EXAMPLES OF NEIGHBOUR TRANSITIVE CODES

In this section we define four infinite families of codes and prove that all codes in these families are neighbour transitive. We use these codes, in Section 4, to classify X -neighbour transitive codes with $X \leq \text{Diag}_m(S_m) \rtimes \mathfrak{L}$. In all cases $m > 1$.

Definition 3.1. (i) For $a \in Q$ let $\alpha(a) = (a, \dots, a) \in V(\Gamma)$ and define $\text{Rep}(m, q) := \{\alpha(a) : a \in Q\}$, the *repetition code* in $H(m, q)$.

(ii) Let $m < q$, and define

$$\begin{aligned} \text{Diff}(m, q) &:= \{(\alpha_1, \dots, \alpha_m) \in V(\Gamma) : \alpha_i \neq \alpha_j \text{ for } i \neq j\} \\ &= \{\alpha \in V(\Gamma) : \text{Num}(\alpha) = \{(1, m)\}\}. \end{aligned}$$

(iii) Let m be odd with $m \geq 3$ and $q = 2$, and define, in $\Gamma = H(m, 2)$,

$$\begin{aligned} W([m/2], 2) &:= \{\alpha \in V(\Gamma) : \text{wt}(\alpha) = (m \pm 1)/2\} \\ &= \{\alpha \in V(\Gamma) : \text{Num}(\alpha) = \{(1, (m+1)/2), (1, (m-1)/2)\}\}. \end{aligned}$$

(iv) Let p be any positive integer, and let $m = pq$, and define

$$\text{All}(pq, q) := \{\alpha \in V(\Gamma) : \text{Num}(\alpha) = \{(p, q)\}\}$$

Theorem 3.2. *Let C be one of the codes in Definition 3.1. Then C is neighbour transitive, and $\text{Aut}(C) = \text{Diag}_m(S_q) \rtimes \mathfrak{L}$. Moreover, C has minimum distance $\delta = m, 1, 1$ and 2 respectively in (i), (ii), (iii), (iv) of Definition 3.1.*

Proof. It follows from Lemma 2.10 that, in all cases, $\text{Aut}(C)$ contains $L := \text{Diag}_m(S_q) \rtimes \mathfrak{L}$, and it is clear that the minimum distance of C is as stated. Moreover, it is easy to check that the group L acts transitively on C (again in all four cases). Now, the set C_1 of neighbours is

$$C_1 = \begin{cases} \{\nu(\alpha(a), i, b) \in V(\Gamma) : 1 \leq i \leq m, a, b \in Q, a \neq b\} & \text{in case (i)} \\ \{(\alpha_1, \dots, \alpha_m) \in V(\Gamma) : \exists \text{ unique } i \neq j \text{ with } \alpha_i = \alpha_j\} & \text{in case (ii)} \\ \{\alpha \in V(\Gamma) : \alpha \text{ has weight } \frac{m-3}{2} \text{ or } \frac{m+3}{2}\} & \text{in case (iii)} \\ \{\alpha \in V(\Gamma) : \text{Num}(\alpha) = \{(p-1, 1), (p, q-2), (p+1, 1)\}\} & \text{in case (iv)} \end{cases}$$

(noting that in case (iv) we may have $q = 2$), and again in all cases it is straight forward to check that L is transitive on C_1 . Thus C is L -neighbour transitive. It remains to prove that $\text{Aut}(C) = L$. Suppose to the contrary that $\text{Aut}(C)$ contains $y = (h_1, \dots, h_m)\sigma$ such that $h_i \neq h_j$ for some $i \neq j$. Since $\mathfrak{L} \leq L \leq \text{Aut}(C)$, we may assume that $\sigma = 1$ and that $h_1 \neq h_2$. Moreover, since $\text{Diag}_m(S_q) \leq \text{Aut}(C)$, we may further assume that $h_2 = 1$, so $h_1 \neq 1$. Let $a, b \in Q$ such that $a^{h_1} = b \neq a$. We consider the cases above separately, and in the first two cases arrive at a contradiction by exhibiting a codeword $\alpha \in C$ such that $\alpha^y \notin C$.

(i) If $C = \text{Rep}(m, q)$ then $\alpha(a)^y|_1 = b$ and $\alpha(a)^y|_2 = a$, so $\alpha(a)^y \notin C$.

(ii) If $C = \text{Diff}(m, q)$, then C contains a codeword α with $\alpha_1 = a$ and $\alpha_2 = b$. However, α^y has $(\alpha^y)|_1 = (\alpha^y)|_2 = b$, so $\alpha^y \notin C$.

(iii) Let $q = 2$, $C = W([m/2], 2)$ with $m \geq 3$ and m odd, and consider

$$C' = \text{Rep}(m, 2) = \{\mathbf{0} = (0, \dots, 0), \mathbf{1} = (1, \dots, 1)\}.$$

Let $\alpha \in V(\Gamma)$ such that $\text{wt}(\alpha) = k$ for $1 \leq k \leq m-1$. Then $d(\alpha, \mathbf{0}) = k$ and $d(\alpha, \mathbf{1}) = m-k$. If $k \leq (m-1)/2$, then $k \leq m-1-k < m-k$, and so $d(\alpha, C') = k$. If $k \geq (m+1)/2$, then $k \geq m+1-k > m-k$, and so $d(\alpha, C') = m-k$. It follows that $d(\alpha, C')$ is maximised when $k = (m-1)/2$ or $k = (m+1)/2$, and in both cases $d(\alpha, C') = (m-1)/2$. Thus C' has covering radius $\rho = (m-1)/2$. It also follows that

$$C'_\rho = W([m/2], 2) = C.$$

It is known that C' is completely transitive and hence completely regular [5, Example 2.5]. Moreover, we have just proved that $\text{Aut}(C') = \text{L}$. Therefore, by Lemma 2.9, $\text{Aut}(C) = \text{Aut}(C') = \text{L}$.

(iv) Let $\nu \in V(\Gamma)$ and suppose $Q(\nu) = \{(a_1, p_1), \dots, (a_k, p_k)\}$ with $p_1 \geq p_2 \geq \dots \geq p_k$. Then $k \leq q$ and $p_1 + \dots + p_k = m = pq$, in particular, $p_1 \geq p$. There exists $\sigma \in \mathfrak{L} \leq \text{Aut}(C)$ such that $\nu^\sigma = (a_1^{p_1}, a_2^{p_2}, \dots, a_k^{p_k})$. Consider the codeword $\alpha = (a_1^p, a_2^p, \dots, a_q^p) \in C$. Then ν^σ and α agree in at least the first p entries. Therefore $d(\nu^\sigma, \alpha) \leq (p-1)q$ and so $d(\nu, C) = d(\nu^\sigma, C) \leq (p-1)q$. Therefore $\rho \leq (p-1)q$. Now consider $\nu = (a, \dots, a)$ for some $a \in Q$. It follows from the definition of C that $d(\nu, \alpha) = (p-1)q$ for all $\alpha \in C$. Therefore $d(\nu, C) = (p-1)q$ and so $\rho = (p-1)q$. Moreover, $\text{Rep}(m, q) \subseteq C_\rho$. Now suppose $\nu \in C_\rho$ and $Q(\nu) = \{(a_1, p_1), \dots, (a_k, p_k)\}$ with $k \geq 2$ and $p_1 \geq p$. There exists $\sigma \in \mathfrak{L} \leq \text{Aut}(C)$ such that $\nu^\sigma = (a_1^p, a_2^{p_2}, a_1^{p_1-p}, a_3^{p_3}, \dots, a_k^{p_k})$. Since $\sigma \in \text{Aut}(C)$, Lemma 2.6 implies that $\nu^\sigma \in C_\rho$ also. Consider the codeword $\alpha = (a_1^p, a_2^p, \dots, a_q^p)$. Then ν^σ and α agree in the first $p + p_2 > p$, therefore $d(\nu^\sigma, \alpha) \leq pq - (p+1) < (p-1)q$, which is a contradiction as $\nu^\sigma \in C_\rho$. It follows that $C_\rho = \text{Rep}(m, q)$. In particular, by Lemma 2.6, $\text{Aut}(C)$ leaves $\text{Rep}(m, q)$ invariant and so $\text{Aut}(C)$ is contained in $\text{Aut}(\text{Rep}(m, q))$, which we have just proved is equal to L . \square

The proof of Theorem 3.2 yields the following immediate corollary.

Corollary 3.3. (i) If $q = 2$ and m is odd, $m \geq 3$, then $C = W([m/2], 2)$ has covering radius $\rho = (m-1)/2$ and $C_\rho = \text{Rep}(m, 2)$; both C and C_ρ are completely transitive.

(ii) If $m = pq$ for some p , then $C = \text{All}(pq, q)$ has covering radius $\rho = (p-1)q$ and $C_\rho = \text{Rep}(m, q)$.

4. CHARACTERISING A FAMILY OF NEIGHBOUR TRANSITIVE CODES

In this section we characterise X -neighbour transitive codes with $X \leq \text{Diag}_m(S_q) \rtimes \mathfrak{L}$. However, before we consider such codes, we first prove some interesting results about connected subsets Δ of vertices of $\Gamma = H(m, q)$ (that is to say, the subgraph of Γ induced on Δ is connected).

Lemma 4.1. Let Δ be a connected subset of $V(\Gamma)$. Let C be a code that is a proper subset of Δ . Then $C_1 \cap \Delta \neq \emptyset$.

Proof. Let $\alpha \in C$ and $\beta \in \Delta \setminus C$. Since Δ is a connected subset, there exists a path

$$\alpha = \alpha_0, \alpha_1, \dots, \alpha_\ell = \beta$$

such that each $\alpha_i \in \Delta$. Because $\alpha \in C$ and $\beta \notin C$, there is a least $i < \ell$ such that $\alpha_i \in C$ and $\alpha_{i+1} \notin C$. Since $d(\alpha_i, \alpha_{i+1}) = 1$, it follows that $\alpha_{i+1} \in C_1$. \square

We now prove that some of the codes in Definition 3.1 are connected subsets of $V(\Gamma)$.

Lemma 4.2. *The codes $\text{Diff}(m, q)$ (with $1 < m < q$) and $W([m/2], 2)$ (with m odd and $m \geq 3$) are connected subsets of $V(\Gamma)$.*

Proof. Firstly we consider $\Delta_1 = \text{Diff}(m, q)$. Let $\alpha, \beta \in \Delta_1$. We shall prove that α, β are connected by a path in Δ_1 using induction on the distance $d(\alpha, \beta)$ in Γ . This is true if $d(\alpha, \beta) = 1$, so assume that $d(\alpha, \beta) = w > 1$, and the property holds for distances less than w . Let $S = \{k : \alpha_k = \beta_k\}$, $i \in M \setminus S$ and $\alpha^* = \nu(\alpha, i, \beta_i)$. Then α^* is adjacent to α in Γ . If $\beta_i \neq \alpha_k$ for all $k \in M \setminus (S \cup \{i\})$, then $\alpha^* \in \Delta_1$ and $d(\alpha^*, \beta) = w - 1$. Therefore, by the inductive hypothesis, α^* and β are connected by a path in Δ_1 and hence so are α and β . Thus we may assume that $\beta_i = \alpha_j$ for some $j \in M \setminus (S \cup \{i\})$. We note that j is unique since $\alpha \in \Delta_1$. Also $\alpha_j^* = \alpha_i^*$ and so $\alpha^* \notin \Delta_1$. Since $m < q$, there exists $a \in Q \setminus \{\alpha_1, \dots, \alpha_m\}$. Let $\alpha^\diamond = \nu(\alpha, j, a)$. Then $\alpha^\diamond \in \Delta_1 \cap \Gamma_1(\alpha)$. If $a = \beta_j$ then $d(\alpha^\diamond, \beta) = w - 1$. Therefore, by the inductive hypothesis, α^\diamond and β are connected by a path in Δ_1 and hence so are α and β . If $a \neq \beta_j$ then $d(\alpha^\diamond, \beta) = w$. In this case let $\alpha^\heartsuit = \nu(\alpha^\diamond, i, \beta_i)$. It follows that $\alpha^\heartsuit \in \Delta_1 \cap \Gamma_1(\alpha^\diamond)$ and $d(\alpha^\heartsuit, \beta) = w - 1$. Therefore by the inductive hypothesis, α^\heartsuit and β are connected by a path in Δ_1 and hence so are α and β . Thus Δ_1 is connected by induction.

We now consider the set $\Delta_2 = W([m/2], 2)$. Let $\alpha, \beta \in \Delta_2$. We prove α, β are connected by a path in Δ_2 using induction on $d(\alpha, \beta)$ in Γ . This is true if $d(\alpha, \beta) = 1$, so assume that $d(\alpha, \beta) = w > 1$, and the property holds for distances less than w . Recall from Definition 2.2 the sets $S(\alpha, \beta)$, $J(\alpha, \beta)$ and $D(\alpha, \beta)$. Because $H(m, 2)$ consists of binary vertices, it follows that $D(\alpha, \beta) = \emptyset$, and so $\text{supp}(\alpha) = S(\alpha, \beta) \cup J(\alpha, \beta)$, $\text{supp}(\beta) = S(\alpha, \beta) \cup J(\beta, \alpha)$, and by Lemma 2.3, $d(\alpha, \beta) = |J(\alpha, \beta)| + |J(\beta, \alpha)|$. If α has weight $\frac{m+1}{2}$ then $J(\alpha, \beta) \neq \emptyset$. Similarly, if α has weight $\frac{m-1}{2}$ then $J(\beta, \alpha) \neq \emptyset$. Let $i_1 \in J(\alpha, \beta)$, $i_2 \in J(\beta, \alpha)$ if α has weight $\frac{m+1}{2}$, $\frac{m-1}{2}$ respectively. Let α^* be the vertex whose support consists of the following set:

$$\text{supp}(\alpha^*) = \begin{cases} \text{supp}(\alpha) \setminus \{i_1\} & \text{if } \alpha \text{ has weight } \frac{m+1}{2} \\ \text{supp}(\alpha) \cup \{i_2\} & \text{if } \alpha \text{ has weight } \frac{m-1}{2} \end{cases}$$

Clearly $\alpha^* \in \Gamma_1(\alpha)$. Moreover, α^* has weight $\frac{m-1}{2}$, $\frac{m+1}{2}$ if α has weight $\frac{m+1}{2}$, $\frac{m-1}{2}$ respectively. Thus $\alpha^* \in \Delta_2$. Also, $J(\alpha^*, \beta) = J(\alpha, \beta) \setminus \{i_1\}$ and $J(\beta, \alpha^*) = J(\beta, \alpha)$ if α has weight $\frac{m+1}{2}$. Similarly, $J(\beta, \alpha^*) = J(\beta, \alpha) \setminus \{i_2\}$ and $J(\alpha^*, \beta) = J(\alpha, \beta)$ if α has weight $\frac{m-1}{2}$. Thus, by Lemma 2.3, we deduce that $d(\alpha^*, \beta) = w - 1$. By our inductive hypothesis α^* and β are connected by a path in Δ_2 and hence so are α and β . This completes the proof by induction. \square

Theorem 4.3. *Let C be an X -neighbour transitive code in $H(m, q)$ such that $X \leq \text{Diag}_m(S_q) \rtimes \mathfrak{L}$. Then one of the following holds:*

- (i) $C = \{(a, \dots, a)\}$ for some $a \in Q$;
- (ii) $C = \text{Rep}(m, q)$;
- (iii) $C = \text{Diff}(m, q)$ where $m < q$;

- (iv) $C = W([m/2], 2)$ where $m \geq 3$ and odd;
- (v) there exists a positive integer p such that $m = pq$ and C is contained in $\text{All}(pq, q)$.

Proof. Let $\alpha \in C$ and suppose that α has composition

$$Q(\alpha) = \{(a_1, p_1), \dots, (a_k, p_k)\}$$

with $p_1 \geq p_2 \geq \dots \geq p_k$ and $k \leq q$. Let $L := \text{Diag}_m(S_q) \rtimes \mathfrak{L}$. We break our analysis up into the cases where $k = 1$ and $k \geq 2$.

Case $k = 1$: In this case $\alpha = (a_1, \dots, a_1)$ and

$$C = \alpha^X \subseteq \alpha^L = \text{Rep}(m, q).$$

If $|C| = 1$, then $X \leq L_\alpha = \text{Diag}_m(S_{q-1}) \rtimes \mathfrak{L}$ and $C_1 = \{\nu(\alpha, i, b) : 1 \leq i \leq m, b \in Q \setminus \{a_1\}\}$. As L_α fixes setwise C and C_1 , and is transitive on both, it follows that C is L_α -neighbour transitive. By the above reduction we only find $C = \{(a_1, \dots, a_1)\}$, but of course the examples here are $\{(a, \dots, a)\}$ for all $a \in Q$, as in (i). Suppose now that $|C| \geq 2$. Since $C \subseteq \text{Rep}(m, q)$ it follows that $\delta = m$. By Remark 2.8, C is 1-regular, and because $\delta = m$, C is equivalent to $\text{Rep}(m, q)$ by [5, Lemma 2.15]. Thus $|C| = q$ and $C = \text{Rep}(m, q)$, as in (ii).

Case $k \geq 2$: Suppose first that $p_1 = 1$. Then $k = m$ and

$$\alpha \in \hat{C} = \begin{cases} \text{All}(q, q) & \text{if } m = q \\ \text{Diff}(m, q) & \text{if } m < q. \end{cases}$$

Since L fixes \hat{C} and $X \leq L$, we have that $C = \alpha^X \subseteq \alpha^L = \hat{C}$. If $m = q$ then (v) holds. Thus assume that $m < q$ and $\hat{C} = \text{Diff}(m, q)$. In this case, C_1 contains $\nu = \nu(\alpha, m, \alpha_1)$ and $\text{Num}(\nu) = \{(2, 1), (1, m-2)\}$. By Corollary 2.11, $\text{Num}(\nu') = \text{Num}(\nu)$ for all $\nu' \in C_1$, and in particular, $C_1 \cap \hat{C} = \emptyset$. If C is a proper subset of \hat{C} then, by Lemmas 4.1 and 4.2, we have that $C_1 \cap \hat{C} \neq \emptyset$, which is a contradiction. Thus $C = \text{Diff}(m, q)$ and (iii) holds.

We can now assume that $p_1 \geq 2$. As S_m acts m -transitively, there exists $\sigma \in \mathfrak{L}$ such that $\alpha^\sigma = (a_1^{p_1}, \dots, a_k^{p_k}) \in C^\sigma$. By Lemma 2.6, C^σ is $(\sigma^{-1}X\sigma)$ -neighbour transitive, and as $\text{Diag}_m(S_q)$ is centralised by \mathfrak{L} , it follows that $\sigma^{-1}X\sigma \leq L$. Let $\bar{X} = \sigma^{-1}X\sigma$, $\bar{\alpha} = \alpha^\sigma$ and $\bar{C} = C^\sigma$. Suppose that $k < q$. Then $q \geq 3$ and there exists $a \in Q$ that does not occur in $\bar{\alpha}$. Consider $\nu_1 = (a, a_1^{(p_1-1)}, a_2^{p_2}, \dots, a_k^{p_k})$ and $\nu_2 = (a_1^{(p_1+1)}, a_2^{(p_2-1)}, \dots, a_k^{p_k})$, which are both adjacent to $\bar{\alpha}$. Then $\text{Num}(\nu_1)$, $\text{Num}(\nu_2)$ and $\text{Num}(\bar{\alpha})$ are pairwise distinct, which is a contradiction to Corollary 2.11. Thus $k = q$. If $p_j = p_1$ for all j , then $m = pq$ (where $p = p_1$) and $\text{Num}(\bar{\alpha}) = \{(p, q)\}$. Thus $\bar{\alpha} \in \text{All}(pq, q)$ and

$$\bar{C} = \bar{\alpha}^{\bar{X}} \subseteq \bar{\alpha}^L = \text{All}(pq, q).$$

As $\sigma \in \text{Aut}(\text{All}(pq, q))$, it follows that $C = \bar{C}^{\sigma^{-1}} \subseteq \text{All}(pq, q)$ and (v) holds. Thus we now assume that $p_1 > p_k$. Let t be minimal such that $p_1 > p_t$, that is, $p := p_1 = p_2 = \dots = p_{t-1} > p_t$, and note that $t \geq 2$. Define $\nu_1 \in \Gamma_1(\bar{\alpha})$ by

$$\nu_1 = \begin{cases} (a_1^p, \dots, a_{t-2}^p, a_{t-1}^{p+1}, a_t^{p_t-1}, \dots, a_q^{p_q}) & \text{if } t \geq 3 \\ (a_1^{p+1}, a_t^{p_t-1}, a_{t+1}^{p_t+1}, \dots, a_q^{p_q}) & \text{if } t = 2 \end{cases}$$

TABLE 1. Neighbours of $\bar{\alpha}$

Line	Case	$\nu_2 \in \Gamma_1(\bar{\alpha})$
1	$t > 2$	$(a_1^{p+1}, a_2^{p-1}, a_3^p, \dots, a_{t-1}^p, a_t^{p_t}, \dots, a_q^{p_q})$
2	$t = 2, p_2 \leq p - 2$	$(a_1^{p-1}, a_2^{p_2+1}, a_3^{p_3}, \dots, a_q^{p_q})$
3	$t = 2, p_2 = p - 1, q \geq 3$	$(a_1^p, a_2^p, a_3^{p_3-1}, \dots, a_q^{p_q})$

and note that $(p+1, 1) \in \text{Num}(\nu_1)$ for all t , and $(p, t-2) \in \text{Num}(\nu_1)$ if $t \geq 3$, while no element of $\text{Num}(\nu_1)$ has first entry p if $t = 2$. As $(p, t-1) \in \text{Num}(\bar{\alpha})$ it follows that $\text{Num}(\nu_1) \neq \text{Num}(\bar{\alpha})$, and so Corollary 2.11 implies that $\nu_1 \in \bar{C}_1$. We claim that $t = 2$, $p_t = p_2 = p - 1$ and $q = 2$.

Assume to the contrary that the claim is false. Then t, p_2, q satisfy the conditions in column 2 of Table 1 for exactly one of the lines. For each line of Table 1, let ν_2 be the vertex in column 3. In each case $\nu_2 \in \Gamma_1(\bar{\alpha})$ and $\text{Num}(\nu_2) \neq \text{Num}(\bar{\alpha})$. We also have that $\text{Num}(\nu_1) \neq \text{Num}(\nu_2)$: this is clear in lines 2 and 3 since then no element of $\text{Num}(\nu_2)$ has first entry $p+1$, while in line 1, $(p, t-3) \in \text{Num}(\nu_2)$ if $t > 3$ and no entry of $\text{Num}(\nu_2)$ has first entry p if $t = 3$. Since $\text{Num}(\nu_2) \neq \text{Num}(\bar{\alpha})$, it follows from Corollary 2.11 that $\nu_2 \in C_1$. However, Corollary 2.11 then implies that $\text{Num}(\nu_2) = \text{Num}(\nu_1)$, which is a contradiction. Thus the claim is proved. As $t = 2$, $p_2 = p - 1$ and $q = 2$, it follows that $m = 2p - 1 \geq 3$ and $\bar{\alpha} = (a_1^p, a_2^{p-1})$. By identifying Q with $\{0, 1\}$, it follows that $\bar{\alpha}$ has weight $p = \frac{m+1}{2}$ or $p-1 = \frac{m-1}{2}$, and therefore so does $\alpha = \bar{\alpha}^{\sigma^{-1}}$, since $\sigma \in \mathfrak{L}$. Thus $\alpha \in W([m/2], 2)$ and

$$C = \alpha^X \subseteq \alpha^L = W([m/2], 2).$$

Let $\nu \in \Gamma_1(\alpha)$. Then ν has weight $\frac{m+3}{2}$ or $\frac{m-3}{2}$ and $\text{Num}(\nu) = \{(1, \frac{m+3}{2}), (1, \frac{m-3}{2})\}$. Thus $\text{Num}(\nu) \neq \text{Num}(\alpha)$ and Corollary 2.11 implies that $\nu \in C_1$. Hence Corollary 2.11 implies that $\text{Num}(\nu') = \text{Num}(\nu)$ for all $\nu' \in C_1$, in particular $C_1 \cap W([m/2], 2) = \emptyset$. If C is a proper subset of $W([m/2], 2)$ then, by Lemmas 4.1 and 4.2, $C_1 \cap W([m/2], 2) \neq \emptyset$, which is a contradiction. Thus $C = W([m/2], 2)$ and (iv) holds. \square

Remark 4.4. Theorem 4.3 gives us a proof of Theorem 1.1. None of the codes in cases (i)–(iv) of Theorem 4.3 are constant composition codes, and any subset of $\text{All}(pq, q)$ is necessarily a frequency permutation array.

5. ACKNOWLEDGEMENTS

This research for the first author was supported by an Australian Postgraduate Award and by the Australian Research Council Federation Fellowship FF0776186 of the second author.

REFERENCES

- [1] Brouwer, A.E., Cohen, A.M., Neumaier, A.: Distance-regular graphs, *Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)]*, vol. 18. Springer-Verlag, Berlin (1989)
- [2] Chu, W., Colbourn, C.J., Dukes, P.: Constructions for permutation codes in powerline communications. *Des. Codes Cryptogr.* **32**(1-3), 51–64 (2004). DOI 10.1023/B:DESI.0000029212.52214.71

- [3] Chu, W., Colbourn, C.J., Dukes, P.: On constant composition codes. *Discrete Appl. Math.* **154**(6), 912–929 (2006). DOI 10.1016/j.dam.2005.09.009
- [4] Gillespie, N., Praeger, C.: Neighbour transitivity on codes in Hamming graphs. *Des. Codes Cryptogr.* (to appear). DOI 10.1007/s10623-012-9614-5
- [5] Gillespie, N.I., Giudici, M., Praeger, C.E.: Classification of a family of completely transitive codes. Preprint (2012)
- [6] Giudici, M., Praeger, C.E.: Completely transitive codes in Hamming graphs. *European J. Combin.* **20**(7), 647–661 (1999). DOI 10.1006/eujc.1999.0313
- [7] Han Vinck, A.J.: Coded modulation for power line communications. *AEÜ Journal* **Jan**, 45–49 (2000). arXiv:1104.4528v1
- [8] Huczynska, S., Mullen, G.L.: Frequency permutation arrays. *J. Combin. Des.* **14**(6), 463–478 (2006). DOI 10.1002/jcd.20096
- [9] Neumaier, A.: Completely regular codes. *Discrete Math.* **106/107**, 353–360 (1992). DOI 10.1016/0012-365X(92)90565-W. A collection of contributions in honour of Jack van Lint
- [10] Pavlidou, N., Han Vinck, A., Yazdani, J., Honary, B.: Power line communications: state of the art and future trends. *Communications Magazine, IEEE* **41**(4), 34 – 40 (2003). DOI 10.1109/MCOM.2003.1193972
- [11] Pless, V.: Introduction to the theory of error-correcting codes, third edn. Wiley-Interscience Series in Discrete Mathematics and Optimization. John Wiley & Sons Inc., New York (1998). A Wiley-Interscience Publication

[GILLESPIE AND PRAEGER] CENTRE FOR MATHEMATICS OF SYMMETRY AND COMPUTATION, SCHOOL OF MATHEMATICS AND STATISTICS, THE UNIVERSITY OF WESTERN AUSTRALIA, 35 STIRLING HIGHWAY, CRAWLEY, WESTERN AUSTRALIA 6009

E-mail address: neil.gillespie@graduate.uwa.edu.au, cheryl.praeger@uwa.edu.au